P⬤RTAL

USPTO

Search: ⦿ The ACM Digital Library　○ The Guide

instructions validate concealed signature　　　　　　　SEARCH

Searching within **The ACM Digital Library** for: instructions validate concealed signature　(start a n

Found **5** of **249,200**

REFINE YOUR SEARCH

▼ Refine by Keywords

instructions validate co

SEARCH

Discovered Terms

▼ Refine by People
Names
Institutions
Authors

▼ Refine by
Publications
Publication Year
Publication Names
ACM Publications
All Publications
Publishers

▼ Refine by
Conferences
Sponsors
Events
Proceeding Series

ADVANCED SEARCH
🔍 Advanced Search

FEEDBACK
✎ Please provide us
with feedback

Found **5** of **249,200**

Search Results　　　　　Related SIGs　　Related Conferences

Results 1 - 5 of 5　　　　　　　　　　　Sort by | relevance ▼ | in | e

◆ Save results to a Binder

1　Architecture for Protecting Critical Secrets in Microprocessors
◆ Ruby B. Lee, Peter C. S. Kwan, John P. McGregor, Jeffrey Dwoskin, Zhenghd
June 2005 **ISCA '05:** Proceedings of the 32nd annual international sympos
　　　Architecture
Publisher: ACM

Full text available: 📄 Pdf (143.62 KB)　Additional Information: full citation, abstract, referen
　　　　　　　　　　　　　　　　　　　　　　　terms

Bibliometrics: Downloads (6 Weeks): 16,　Downloads (12 Months): 110,　Citatio

We propose "secret-protected (SP)" architecture to enable secure and c
protection of critical secrets for a given user in an on-line environment.
examples of critical secrets, and key protection and management is a fu
problem ...

Also published in:
　May 2005 **SIGARCH Computer Architecture News** Volume 33 Issue 2

2　Security as a new dimension in embedded system design
◆ Paul Kocher, Ruby Lee, Gary McGraw, Anand Raghunathan / Srivaths Ravi
June 2004 **DAC '04:** Proceedings of the 41st annual conference on Design ;
Publisher: ACM

Full text available: 📄 Pdf (209.10 KB)　Additional Information: full citation, abstract, referen
　　　　　　　　　　　　　　　　　　　　　　terms

Bibliometrics: Downloads (6 Weeks): 76,　Downloads (12 Months): 472,　Citatio

The growing number of instances of breaches in information security in
years has created a compelling case for efforts towards secure electroni
Embedded systems, which will be ubiquitously used to capture, store, m
and ...

Keywords: PDAs, architectures, battery life, cryptography, design, des
methodologies, digital rights management, embedded systems, perform
security processing, security protocols, sensors, software attacks, tamp
trusted computing, viruses

**3　SHARK: Architectural support for autonomic protection against stealt
exploits**
Vikas R. Vasisht, Hsien-Hsin S. Lee
November 2008 **MICRO '08: Proceedings of the 2008 41st IEEE/ACM I
Symposium on Microarchitecture - Volume 00**, Volume (

Publisher: IEEE Computer Society

Full text available: Pdf (538.23 KB) Additional Information: full citation, abstract

Bibliometrics: Downloads (6 Weeks): 23, Downloads (12 Months): 23, Citation

Rootkits have become a growing concern in cyber-security. Typically, th
vulnerabilities to gain root privileges of a system and conceal malware's
users and system administrators without any authorization. Once infect

4 Using dynamic information flow analysis to detect attacks against ap

Wes Masri, Andy Podgurski

July 2005 **SESS '05**: Proceedings of the 2005 workshop on Software engin
systems—building trustworthy applications

Publisher: ACM

Full text available: Pdf (243.45 KB) Additional Information: full citation, abstract, referen
terms

Bibliometrics: Downloads (6 Weeks): 7, Downloads (12 Months): 89, Citation

This paper presents a new approach to using dynamic information flow
attacks against application software. The approach can be used to revea
some conditions, to prevent attacks that violate a specified information

Keywords: Computer security, dynamic information flow analysis, intru
observation-based testing, program dependences

Also published in:
July 2005 **SIGSOFT Software Engineering Notes** Volume 30 Issue 4

5 Practical secrecy-preserving, verifiably correct and trustworthy auctic

D. C. Parkes, M. O. Rabin, S. M. Shieber, C. A. Thorpe

August 2006 **ICEC '06**: Proceedings of the 8th international conference on I
commerce: The new e-commerce: innovations for conquering
obstacles and limitations to conducting successful business on

Publisher: ACM

Full text available: Pdf (507.45 KB) Additional Information: full citation, abstract, referen
terms

Bibliometrics: Downloads (6 Weeks): 4, Downloads (12 Months): 59, Citation

We present a practical system for conducting sealed-bid auctions that p
secrecy of the bids while providing for verifiable correctness and trustw
auction. The auctioneer must accept all bids submitted and follow the pi